Feasibility of Quantum Cryptography with AES for Secure Communication

Proceedings - 2025 10th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2025 • Conference Paper • 2025 •
DOI: 10.1109/ICT4M68001.2025.11363503

Binti Mustaffa, Nurul Muzfirah ; Balqis Binti Mat Daud, Nurulain ; Sase, Takumi

International Islamic University Malaysia, Department of Computer Science, Kuala Lumpur, Malaysia

Abstract

Traditional encryption techniques face serious threats from the rapid development of quantum computing, which could soon compromise many classical algorithms. To address this, new quantum-resistant security methods are needed to protect private data and communications. This paper proposes a hybrid encryption approach that integrates quantum key distribution (QKD) with a simplified 3×3 advanced encryption standard (AES) key matrix, creating a lightweight system. The objective is to provide an efficient encryption method suitable for devices with limited processing power, such as IoT devices. The model was simulated using Qiskit, achieving an average quantum bit error rate of 0.00%, protocol efficiency of 49.72 %, and quantum fidelity of 1.000 under certain conditions. During eavesdropping scenarios, the error rate increased to 16.90 %. The simplified AES achieved a 50.14 % avalanche effect and an encryption time of 0.3073 ms, reducing latency by 17 %

compared to standard AES. These results suggest that combining QKD with lightweight AES can provide quantum resilience and computational efficiency, offering a practical solution for secure communication in the post-quantum era. © 2025 IEEE.

Author keywords

AES; Hybrid Encryption; IoT Security; Qiskit; Quantum Key Distribution

Indexed keywords

Engineering controlled terms

Bit error rate; Computational efficiency; Data privacy; Encryption algorithms; Network security; Quantum communication; Quantum computers; Quantum cryptography; Quantum efficiency; Quantum theory; Security systems

Engineering uncontrolled terms

Advanced Encryption Standard; Encryption technique; Hybrid encryption; IoT security; Key distribution; Private data; Qiskit; Quantum Computing; Quantum key; Security methods

Engineering main heading

Secure communication

Corresponding authors

Corresponding author	N.M. Binti Mustaffa
Affiliation	International Islamic University Malaysia, Department of Computer Science, Kuala Lumpur, Malaysia
Email address	nurulmuzfirah03@gmail.com

Abstract

Author keywords

Indexed keywords

Corresponding authors

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER